(12) UK Patent Application (19) GB (11) 2 360 677 (13) A

(43) Date of A Publication 26.09.2001

(21) Application No 0007162.1

(22) Date of Filing 25.03.2000

(51) INT CL[7]
H04L 9/08 , G06F 1/00 , H04L 9/32

(52) UK CL (Edition S)
H4P PDCSP

(56) Documents Cited
GB 2341061 A EP 0940675 A1 EP 0565281 A2
EP 0194839 A2 US 5809140 A US 5778071 A
US 5638444 A US 5606615 A

(58) Field of Search
UK CL (Edition R) G4A AAP , H4P PDCSA PDCSP
INT CL[7] G06F 1/00 , H04L 9/08 9/32
Online: EPODOC, JAPIO, WPI

(71) Applicant(s)
Pilot Systems (London) Ltd
(Incorporated in the United Kingdom)
10 Barley Mow Passage, Chiswick, LONDON, W4 4PH,
United Kingdom

(72) Inventor(s)
Nigel Orchard

(74) Agent and/or Address for Service
Saunders & Dolleymore
9 Rickmansworth Road, WATFORD, Herts, WD18 0JU,
United Kingdom

(54) Abstract Title
Security system using physical keys containing security algorithms at communicating terminals

(57) Security for transactions between remote terminals 1,2 is provided by having a physical device 4 such as a key, Smart Card or other token at each terminal. This device incorporates an algorithm and sets of such devices have matching algorithms.

In use a random number is generated at one of the terminals and transmitted to the other, the algorithm stored in the security device is applied to the random number at both terminals and the results are compared. Only if the results obtained from applying the algorithm are identical is a transaction enabled.

The connection point for the physical device is incorporated in a mouse in one embodiment.

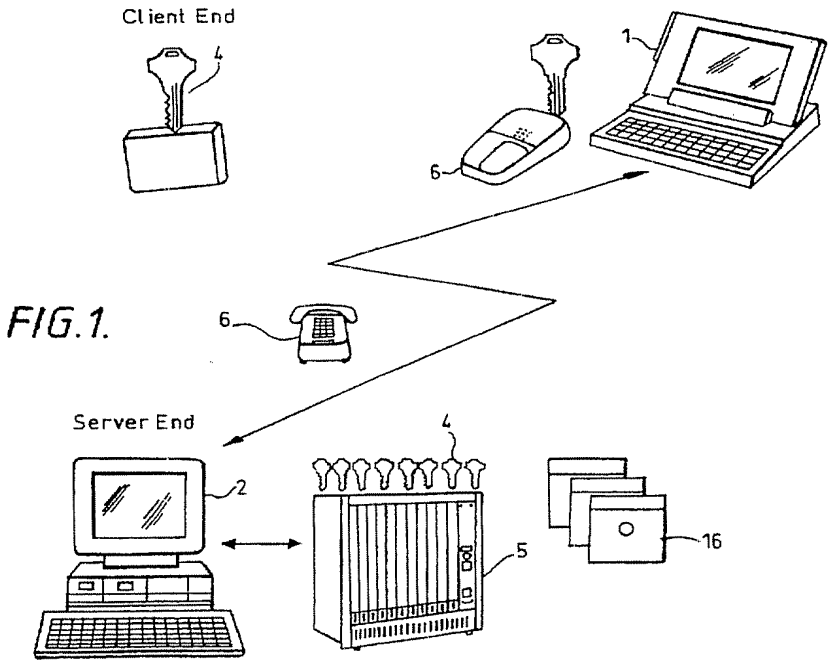

FIG.1.

GB 2 360 677 A

At least one drawing originally filed was informal and the print reproduced here is taken from a later filed formal copy.

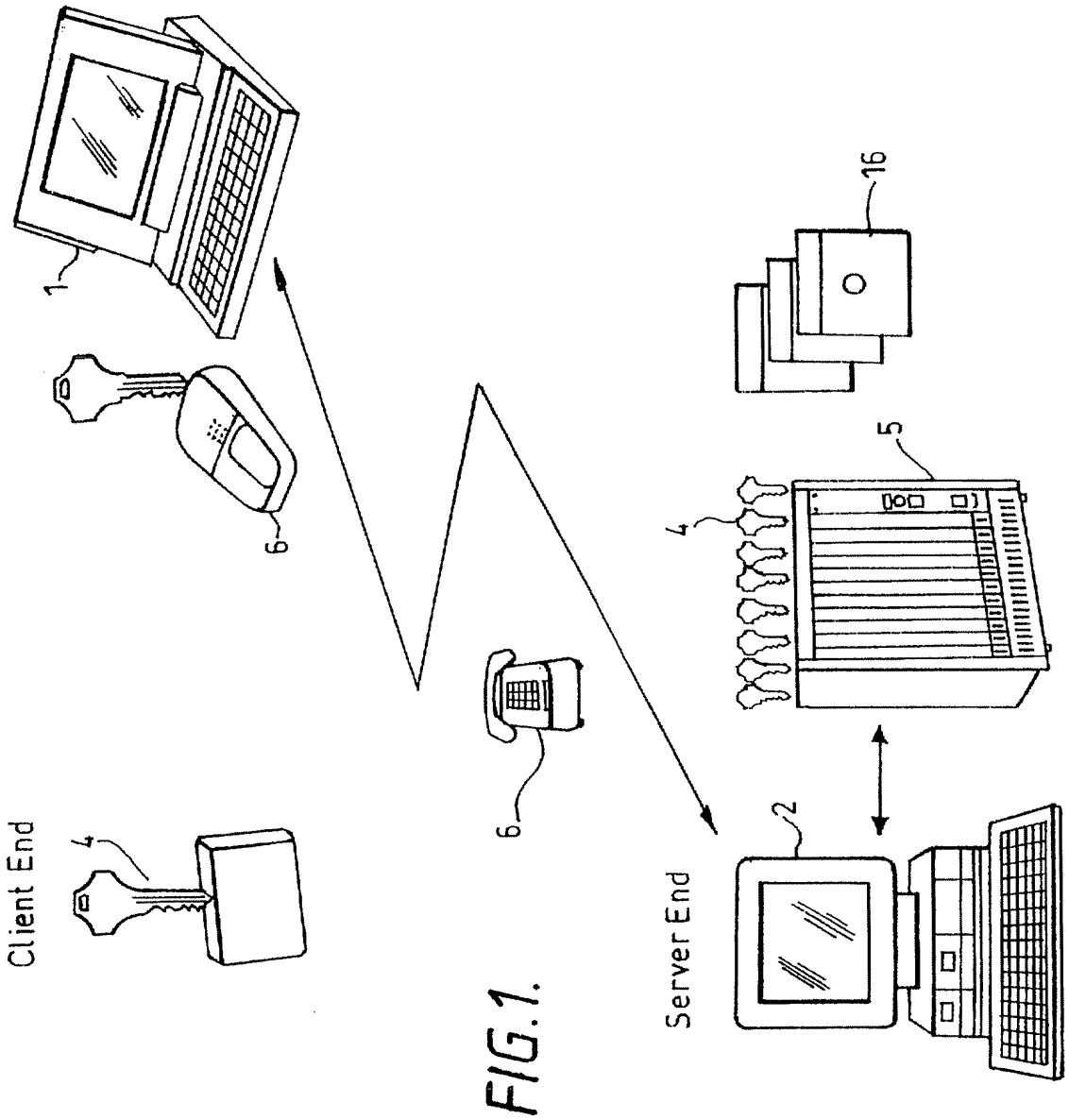

FIG.1.

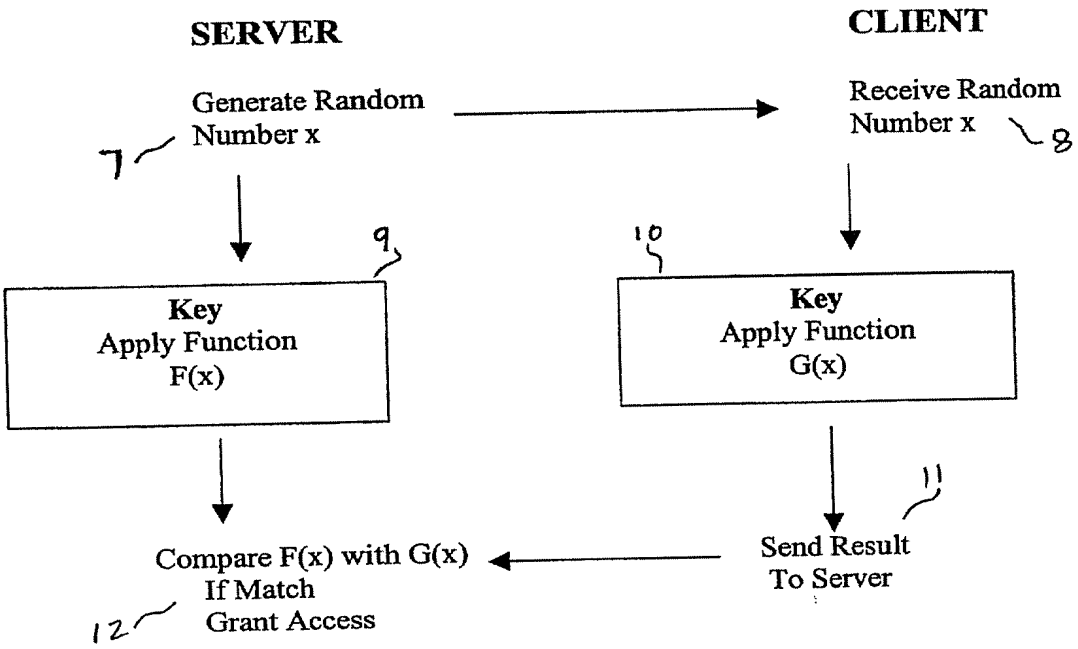
SERVER
CLIENT
Generate Random Number x
7
Receive Random Number x
8
9
10
Key
Apply Function
F(x)
Key
Apply Function
G(x)
11
Send Result To Server
Compare F(x) with G(x)
If Match
Grant Access
12

FIG 2

SECURITY SYSTEM

This invention relates to a security system. In particular, it relates to a security system and method for improving the security of transaction between remote terminals, for example those connected over the Internet, or in a local area network or wide area network, or terminals connected over a telephone system which may be a land based or mobile telephone system, or over a radio system or any other remotely situated terminals.

With the advent and increasing popularity of conducting transactions remotely, particularly on the Internet, and of e-commerce, there is a significant requirement for security. Users need to know that their transactions will be safe and secure and that personal and valuable information, such as credit card numbers, are not allowed to be obtained by unauthorised parties. In particular, both parties in a transaction need to be confident that the other party is indeed who it claims to be.

Various methods of encryption are currently available and software-based systems using public and private keys, pin numbers, represent the current solution to the problem of security. However, many users are still deterred from using e-commerce since the very transparency of most of these methods does not instil confidence.

The present invention arose in an attempt to provide an improved security system for remote and on-line transactions and one which offers immediate reassurance to a user that the other party in a transaction is who it claims to be.

According to the present invention there is provided a security system for providing security for transactions between remote terminals, comprising at least two physical devices, each containing an algorithm; means associated with each

terminal for communicating with the physical device; wherein one of the terminals comprises means for generating a number and forwarding that number to the other terminal, both terminals being adapted to perform said algorithm on said number and, if the result of the algorithm is equal, to enable a transaction to take place.

According to the present invention in a second aspect there is provided a method for providing security for transactions between remote terminals, comprising providing, at each terminal, a physical device incorporating a common algorithm; generating a number at one terminal and transmitting this number to the other terminal; performing the algorithm at both terminals and comparing the result generated by both terminals, whereby only if the result is equal is a transaction enabled.

Preferably, at least one of the physical device is a key provided with an electronically, magnetically or optically stored algorithm.

Preferably, the means for communicating with the key comprises an input device for a computer, preferably a mouse adapted to receive the key and to thereby enable electrical signals to be passed to and/or from the key.

According to the invention in a third aspect there is provided a method for providing security for transactions between remote terminals, comprising providing, at one terminal, a physical device incorporating an algorithm, providing the same algorithm at a second terminal; generating a number at one terminal and transmitting this number to the other terminal; performing the algorithm at both terminals on this number and comparing the result generated by both terminals, whereby only if the result is equal is a transaction enabled.

The invention further provides a method or apparatus including any one or

more of the novel features or steps herein disclosed.

Embodiments of the invention will now be described, by way of example only, with reference to the accompanying drawings in which:

Figure 1 shows schematically a security system; and

Figure 2 shows an authentication method using the apparatus.

Referring to Figure 1, it is becoming more common for users to wish to conduct on-line transactions with remote computer terminals. These can be done over the Internet, using fixed and/or mobile telephone systems and by many other types of systems. Referring to the Figure, there is shown a user's computer terminal 1 in communication with a remote server 2, over a network 3. The server may, for example, be a bank or credit card provider's server or web page. It could also be the web page or the server of any business offering products for on-line retail.

In embodiments of the invention, a user purchases a number of physical keys 4, each of which is substantially identical and which includes electronic processing and/or memory means storing a predefined algorithm. Although each key in the set bears an identical algorithm, each set of keys which a user may purchase will preferably store a different algorithm. If duplication is unavoidable, then this should be such that there is only a very small chance of any two keys having the same algorithm (in the same way that there is only a very small chance that any two mechanical keys can open the same lock). Any desired algorithm may be used in the key and these should preferably be algorithms such that there is a one to one relationship between inputting a number to the algorithm and the result. Functions containing combinations of operations like shift left, shift right, AND, OR, XOR, add, subtract, multiply, divide, mod, square root, raise to the power may be used for example.

The user (client) keeps at least one of the keys 4 and sends one to his service provider (credit card company, etc). The credit provider, at the server end, has a means 5 for receiving each of the keys sent to them by a client and which can transmit data bi-directionally to and from the keys so as to be able to process numbers using the algorithm on each particular key.

The client also has a means into which the key may be input or which can enter into communication with the key, so as also to be able to perform the algorithm, stored on the key, upon a certain number.

In a currently preferred embodiment, the key reader is a computer mouse 6. This can be connected to, for example, the serial port of a computer and includes a slot into which the key can be fitted so that electrical connection is made. Alternatively, the key may link to the mouse, or to any other reader, by any other contact method or wireless (e.g. infrared, radio, etc) method. The mouse may be provided with a slot having electrical contact so that the key can be fitted into the slot and electrical contact be transmitted between the key and the mouse. Bi-directional signals can then be made between the mouse and the computer so that a seed number can be applied from the computer to the key, the algorithm performed upon the number and a result returned.

Although a modified mouse is the preferred embodiment, many other types of readers may be used and the reader may be a separate reader dedicated to this purpose. Alternatively, a slot or other reading means may be provided on the body of the computer 1 itself.

In some embodiments, instead of the user sending a physical key 4 to the server, he may instead send a data storage medium, such as a floppy disc 16, a CD ROM or other disc-type device, a tape or any other physical device to the server so that the algorithm can be used in this manner.

Figure 2 shows one example of a use of the present invention. When a client wishes to conduct a transaction, say a financial transaction with his service provider, he inserts his key 4 into key reader (i.e. mouse) 6. He then initiates a channel of communication (e.g. an Internet connection) with the server and indicates that a transaction is desired to be made. The server at step 7 then generates a number x. This will preferably be a random or pseudo random number but may in principle be any number. This number is sent to the client's computer which receives random number x (8). Both the server and the client then use their key to apply the algorithm (i.e. apply a function) to the number x. Thus, at step 9 the key at the server applies a function F (x).

At around the same time, at the client end the key 4 applies a function G (x) to the number. The result of this is then sent (step 11) back to the server as a number. At step 12, the server compares the results of its own function F (x) with G (x). If the key and the algorithm are the same, then of course the results should be identical. Provided the two numbers generated respectively by the server and by the client are identical, then the client is considered to be authorised and the transaction may be completed.

The present invention accordingly provides a secure manner for authenticating transactions. The algorithm is preferably stored solely on the keys so that it is never available on the client or server's computer for an unauthorised person to access. The algorithm itself is stored on the key in such a manner that its nature cannot be determined or reverse-engineered.

Preferably, each key is only connected at the time of the transaction and at no time is the algorithm actually transmitted electronically between the two stations.

The key preferably has an in-built delay (e.g. 1 second) so that there is a

delay between entering a seed number and receiving the result. This assists in deterring anyone trying to determine the code by feeding in a series of numbers and logging the results. With a built in delay of one second in response, an eight digit seed number would require over 3 years to compile a full list. With a ten digit seed, this would be 300 years or so.

If a user loses his key, or otherwise feels that security has been compromised for any reason, it is a simple matter to "change the locks" by purchasing another set of keys, having a different algorithm, and reissuing keys to the various servers he is using.

Various organisations, such as supermarkets and other retail outlets, may provide sockets associated with their computer systems so that customers who are out and about can still use their key to conduct secure transactions for additional security.

An advantage of the present invention is that the keys are portable and that the customer may carry them around with them and use them in many different places. Present software based encryption systems rely on encryption keys being loaded into user's PC's. Thus, a user cannot conduct secure transactions when he is not at home or has his own portable computer to hand. Thus, suitable sockets may be provided at, for example, Internet cafes, libraries, and other public buildings in association with computers and computer terminals so that users may securely conduct on-line transactions wherever they happen to be.

The present invention establishes identity of users, and therefore there is no need for additional telephone or e-mail contact, or address verification for example.

A separate key unit may be provided which displays the result of an input

number on a screen. This can be for manual use providing identity over the telephone.

The 'key' need not be a physical key, it could be a smart card type device or any other physical token which can store an algorithm which can be used to process a seed number.

Sets of keys may be sold in retail outlets.

The algorithm may be manually generated, or may be generated by a computer program, for example.

An additional security step, such as entry of a PIN, signature recognition, retina or fingerprint scanning, or other step, may be used to improve security even further.

It should be noted that the present invention provides only security and is completely separate from the actual transaction. Once the identities of client and server have been verified, the keys and algorithms play no further part. The interface can be safely published without security being compromised in any way.

In a modification, a third party server may store all the algorithms, either on physical keys or each algorithm could be loaded onto that server, or perhaps transmitted to it by a client. The third party server acts as a verification service, so this verifies that a user is who he claims to be, and sends this verification to the bank's (or other organisation's) server; this need no longer store or have the algorithm locally.

The client may register his algorithm with the third party server, e.g. by dialling in over a dedicated line (preferably not the Internet). The algorithm could

be identified by a plurality (e.g. 5) responses to different seeds, to ensure the correct algorithm is used.

CLAIMS

1. A method for providing security for transactions between remote terminals, comprising providing, at two terminals, a physical device incorporating a common algorithm; generating a number at one terminal and transmitting this number to the other terminal; performing the algorithm at both terminals on this number and comparing the result generated by both terminals, whereby only if the result is equal is a transaction enabled.

2. A method as claimed in Claim 1, wherein one of the terminals serves only to verify a transaction between one of said terminals and a third terminal.

3. A method as claimed in Claim 1 or 2, wherein the user associated with one terminal possesses at least two physical devices bearing the same algorithm and physically sends one of them to the user of the other terminal, prior to any transactions, for use as the physical device at the other terminal.

4. A method as claimed in any preceding claim, wherein the number is generated at said other terminal.

5. A method as claimed in any preceding claim, wherein the physical device is a key provided with a stored algorithm.

6. A method as claimed in Claim 5, wherein the algorithm is stored electronically, magnetically and/or optically on the key.

7. A method as claimed in any preceding claim, further comprising providing a means, associated with each terminal, for communicating with the algorithm on the key, said means comprising a computer input device having means for communicating with the key.

8. A method as claimed in Claim 7, wherein the computer input device comprises a mouse.

9. A method as claimed in Claim 8, wherein the mouse provides a means for electrically connecting with a key.

10. A method as claimed in any preceding claim, wherein the number which is applied to the algorithm is randomly or pseudo-randomly generated.

11. A method as claimed in any preceding claim, wherein the algorithm itself is never transmitted electronically between the two terminals and each physical device is only connected, so that the algorithm can be applied to a number, at the time of a transaction.

12. A method as claimed in any preceding claim, wherein the physical device provides a delay between receiving a number and outputting the results of the algorithm applied to that number.

13. A method for providing security for transactions between remote terminals, comprising providing, at one terminal, a physical device incorporating an algorithm, providing the same algorithm at a second terminal; generating a number at one terminal and transmitting this number to the other terminal; performing the algorithm at both terminals on this number and comparing the result generated by both terminals, whereby only if the result is equal is a transaction enabled.

14. A security system for providing security for transactions between remote terminals, comprising at least two physical devices, each containing a common algorithm; means associated with each terminal for communicating with the physical device; wherein one of the terminals comprises means for generating a

number and forwarding that number to the other terminal, both terminals being adapted to perform said algorithm on said number and, if the results of the algorithm are equal, to enable a transaction to take place.

15. Apparatus as claimed in Claim 14, wherein the physical device is a key provided with an electronically, magnetically and/or optically stored algorithm.

16. Apparatus as claimed in Claim 14 or Claim 15, wherein the means at at least one of the terminals for communicating with the device comprises a computer input device.

17. Apparatus as claimed in Claim 14, wherein the input means comprises a computer mouse adapted to communicate with the physical device.

18. Apparatus as claimed in any of Claims 14 to 17, wherein the physical keys are supplied by a user who sends one of them physically to the user of the other terminal.

19. A method of providing security for transactions between remote terminals substantially as hereinbefore described with reference to, and as illustrated by, the accompanying drawings.

20. Apparatus for providing security for transactions between remote terminals substantially as hereinbefore described with reference to, and as illustrated by, the accompanying drawings.